Kentucky Information Technology Standards (KITS)

Full KITS Report - Word Search

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
5010	Intrusion Detection and Prevention	Products must support approved Enterprise standards in the following categories: • Operating systems—specific Unix operating systems (OSs), MS Windows, Linux • Network topologies—Ethernet, T1/E1 • Switched networks • Protocols—TCP/IP, UDP • Applications—FTP, HTTP, Telnet • Firewalls All tools within this category have the ability to appear to network defense mechanisms as reconnaissance or attack activity. To ensure that the scanning activities are effective, able to complete uninterrupted, and do not raise unnecessary alarm all provisions in CIO-082 Critical Systems Vulnerability Assessments must apply.	A01.011.073	System > Security Management > Intrusion Detection	Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)	Top Layer Products: • IBM ISS Proventia • McAfee Host IPS (included in McAfee Endpoint Protection – Advanced Suite) • McAfee Network Security Manager • McAfee Network Security Platform • Snort-SourceFiret • Suricata • HP TippingPoint Internet Security Systems Products: • RealSecure Server Sensor • RealSecure Site Protector • Retina Network Security Scanner • Symantec Security Monitoring Services • Symantec DeepSight	**Effective:** 6/1/2003 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
5100	Encryption	IETF X.509 Public Key Infrastructure (PKI latest version for digital certificates) The purpose of this standard is to provide Commonwealth of Kentucky agencies guidance on the use of encryption to protect Commonwealth information resources that contain, process, or transmit data classified as sensitive or confidential. This standard applies to encryption controls for data that is at rest (including portable devices and removable media) and data in motion (transmission security). This standard is compatible with, but does not supersede, federal encryption standards. Agencies should refer to the data classifications defined in Enterprise Standard 4080 – Data Classification. https://gotsource.ky.gov/docushare/dsweb/Get/Document-301107/. Once the data has been classified, the agency must determine the proper encryption implementation(s) to achieve the desired level of protection. Encryption Strength - Based on the data classification described above, Commonwealth of Kentucky agencies will use Federal Information Processing Standard (FIPS) 140-2 approved algorithms as outlined in National Institute of Standards and Technology (NIST) 800-57, part 3, Revision 1 for encrypting sensitive and confidential data. Wireless Technologies (including Bluetooth)- COT recommends that organizations with existing legacy IEEE 802.11 implementations develop and implement migration strategies to move to IEEE 802.11i-based security because of its superior security capabilities. IEEE 802.11i addresses the security flaws in the original IEEE 802.11 standard with built-in features	A02.029.342	Application Components > Security Controls > Encryption	Software to convert plaintext to ciphertext through the use of a cryptographic algorithm.	The Entrust suite of PKI enabled products	**Effective:** 7/1/1997 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
5100		providing robust wireless communications security, including support for FIPS 140-2 validated cryptographic algorithms. In addition, it is necessary to employ higher level cryptographic protocols and applications such as Secure Shell (SSH), Transport Layer Security (TLS) or Internet Protocol Security (IPSec) with FIPS 140-2 validated cryptographic modules and associate algorithms to protect sensitive or confidential data in transit. Encryption Key Management Standard - Proper key management is necessary for ensuring that encrypted data is secure and accessible when needed. Procedures should be created, or automated mechanisms utilized, for the management of encryption keys that encompasses the following phases of the Encryption Key Management Life Cycle: • Key creation • Key backup • Key deployment • Key Rotation • Emergency and routine revocation of keying material • Auditing of keying materials and related records • Key recovery • Destruction of revoked or expired keys					

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
5110	Endpoint Storage Device Encryption	Encryption is required by CIO-092 for any portable storage device when it will contain data defined as Sensitive or above according to the Kentucky Data Classification Matrix.	A02.029.342	Application Components > Security Controls > Encryption	Software to convert plaintext to ciphertext through the use of a cryptographic algorithm.	McAfee Endpoint Protection Bitlocker for Microsoft Surface Pro Note: we would like to prevent any new installs of Checkpoint Pointsec	**Effective:** 1/20/2010 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015
5120	Encrypted Flash Drive	An encrypted flash drive is required by CIO-092 when it will contain data defined as sensitive or confidential according to the Kentucky Data Classification Matrix. The encryption will use Federal Information Processing Standard (FIPS) 140-2 approved algorithms as outlined in National Institute of Standards and Technology (NIST) 800-57, part 3, Revision 1 for encrypting sensitive and confidential data.	I01.001.107	Platform > Hardware > Removable Storage Media	Removable storage media is any type of storage device that can be removed from a computer while the system is running.	Any product that utilizes (FIPS) 140-2 approved algorithms as outlined in National Institute of Standards and Technology (NIST) 800-57, part 3, Revision 1 for encrypting sensitive and confidential data.	**Effective:** 2/4/2010 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
5505	Sanitization and Disposal of Information Technology Equipment and Electronic Media	The recognized authority for Sanitization and Disposal standards are the National Institute of Standards and Technology referenced in their documents: • NIST SP 800-53 v. 4: Media Protection • NIST SP 800-88 v. 1: Guidelines for Media Sanitization • NIST SP 800-36: Guide to Selecting Information Technology Security Products, Section 5.9 And U.S. Department of Defense Standard: DoD 5220.22-M: National Industrial Security Program Operating Manual (NISPOM) Archiving Records: Any IT devices (servers, storage, clients), network components, operating system or application software, or storage media containing public records as defined by KRS 61.870(2) and 171.410 shall have the final disposition of those records established with the Kentucky Department for Libraries and Archives prior to disposal through the Division of Surplus Property (Finance) or transfer to other agencies for re-use. CIO-092, Media Protection Policy: This policy ensures proper provisions are in place to protect information stored on media, both digital and non-digital, throughout the media's useful life until its sanitization or destruction. Physical Destruction: Physical destruction is an acceptable option for devices and portable media that are permanently being disposed. On storage devices or media that have been rendered inoperable because of failure, physical destruction is required. See Table 5-1: Sanitization Methods (Destroy Method) for more details on this option.	S03.002.002	Controls > Control Categories > Operational	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people, as opposed to executed by systems. See FIPS 200.	Approved products and mechanisms for rendering data inaccessible depend on the type of media being used and the disposition of the device or media. Further discussion is provided under Technical and Implementation Considerations. Recommended Products: Disks: • WipeDrive • Active@KillDisk Files: • Darik's Boot and Nuke (DBAN) • SecureClean (included with WipeDrive now) Degausser Equipment: • HD-1T Chamber Degausser (Data Security, Inc.) Physical Destruction: • DIsk/Tape Shredder	**Effective:** 2/14/2003 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
5515	Secure Transport	Transport Layer Security (TLS)1.2 or greater encryption is required if data needs to be secured during transmission over inherently unsecure protocols such as FTP, HTTP, SMTP, NNTP, or XMPP (unless the data is encrypted prior to transmission). Secure Shell (SSH) is a Unix/Linux-based command interface and protocol for securely accessing a remote computer. This protocol can be used for remote access as well as secure data transport through SFTP and SCP. All electronic payments (credit card, EFT, etc) and the collection of personally identifiable information must be secured during transport (see Category for Network Services - Electronic Commerce and Payments). Strong encryption (256-bit or greater) is recommended and may be required for certain applications, particularly personal and health-related information as prescribed in federal law or required regulatory compliance. Examples include, but are not limited to PCI (Payment Card Industry) compliance, FISMA (Federal Information Security Management Act), HIPAA (Health Insurance Portability and Accountability Act), FERPA (Family Educational Rights and Privacy Act) and IRS Publication 1075. WS (Web Service) security protocols should be used whenever web services are designed and implemented. To authenticate and secure the web server, a server certificate (digital ID), available from Entrust, must be assigned to the web server. This includes secure servers operated under contract, although any server certificate software may be used in those instances.	S03.002.003	Controls > Control Categories > Technical	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. See FIPS 200.	Entrust.net Transport Layer Security (TLS 1.2) server certificates All web browser approved products (Category 3511) support TLS 1.2 All web server approved products (Category 3510) support TLS 1.2 Secure Shell (SSH), Secure Shell v2 (SSH2)	**Effective:** 6/1/1999 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
5530	Virus Scanning	• All desktops, laptops and servers shall have antivirus/malware protection installed • All systems shall undergo at a minimum a monthly full system scan for viruses and malware • Where possible, portable devices shall also have antivirus protection • Antivrus/anti-malware shall be centrally managed with ongoing updates and reports • End users shall not be able to disable the antvirus/anti-malware software on their systems • Scans should be schedued to occur automatically	A02.029.343	Application Components > Security Controls > Virus Protection	Software used to prevent, detect, and remove self-replicating programs that run and spread by modifying other programs or files.	Windows Server OS: • McAfee Endpoint Protection – Advanced Suite Windows Desktop OS: • McAfee Total Protection for Secure Business Linux OS: • McAfee VirusScan Enterprise for Linux Microsoft Exchange: • McAfee GroupShield for Microsoft Exchange (included in McAfee Security for Email Servers and Microsoft Sharepoint: • McAfee Security for Microsoft Sharepoint NetWare: • McAfee Endpoint Protection – Advanced Suite	**Effective:** 7/1/1997 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015
5545	Spam Filtering	Support for all approved hardware platforms, operating systems software and applications. Ability to detect an unsolicited or inappropriate email and deliver to a separate inbox for review before delivery to the addressee.	A02.029.343	Application Components > Security Controls > Virus Protection	Software used to prevent, detect, and remove self-replicating programs that run and spread by modifying other programs or files.	• McAfee Email Gateway • McAfee Total Protection for Internet Gateways	**Effective:** 8/21/2008 **Revised:** 1/19/2011 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
5550	Web Filtering	• Must be able to analyze domain name • Must be able to break down and analyze web traffic to accurately pinpoint portions of a web page which should not be allowed into the internal network • Must be able to block based on contet • Must be able to be centrally managed	A02.029.343	Application Components > Security Controls > Virus Protection	Software used to prevent, detect, and remove self-replicating programs that run and spread by modifying other programs or files.	• CyBlock (Wavecrest) • McAfee Secure Web Gateway	**Effective:** 1/19/2011 **Revised:** 6/17/2015 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
5700	Firewall	• International Computer Security Association (ICSA) - ICSA Labs® Certification for firewall products • Firewall Product Developers Consortium (FWPD) Product Certification Criteria • Internet Protocol Security Protocol Working Group (IPsec), part of the Internet Engineering Task Force (IETF) • National Institute of Standards and Technology (NIST) Firewall Protection Profile • Support all Internet Protocol (IP) stacks • Approved application servers and operating system (OS) • Integration with internetworking hardware and software from Nortel Networks Based on the enterprise policy CIO-076, COT shall manage all enterprise and intranet firewall and VPN services that utilize the KIH infrastructure. Agencies may manage agency-level Tier II firewall services under certain stipulations and with COT network visibility to the firewall. It is imperative that network services for all agencies within the KIH are protected and that the integrity of the KIH is protected to insure that enterprise services are not compromised. The administration of firewalls and virtual private networks (VPN) is a critical component in securing the KIH infrastructure and computing systems. • Internet and Extranet (business relationships) VPN connections must be managed to maintain enterprise security and reduce security risks. For this reason, COT shall be the approving authority for access to KIH computing resources. Agencies using the Internet to communicate and share data must use the COT-managed VPN service. • Intranet VPN connections shall be managed by COT to maintain enterprise	S03.002.003	Controls > Control Categories > Technical	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. See FIPS 200.	Check Point is the approved product standard for Tier I firewall services. Tier I classification includes all services and/or systems that are considered an enterprise resource. Enterprise resources should be located at the Commonwealth's Data Center (CDC) in order to maximize security benefits and network efficiency. Enterprise resources located at CDC benefit from additional security technologies in place there. Avaya VPN Router firewall product is the enterprise standard for Tier II firewall services. Tier II classification includes all services and/or systems that are agency-specific but available for the enterprise. Agency-specific applications and services would be suitable for Tier II firewall services. Tier II firewall services may not be interoperable with other enterprise security platforms. NOTE: Agencies are encouraged to review the COT security offering for firewall services.	**Effective:** 7/1/1997 **Revised:** 1/19/2011 **Reviewed:** 6/17/2015

EAS Code	EAS Category Name	Standard	KITS Category Code	KITS Domain > Area > Category	KITS Description	Approved Products	Date
5700		security and network routing efficiencies. Agencies wanting to create Intranet VPN's must use COT VPN approved services.					
5710	Desktop / Laptop Firewall Software	• All state-owned laptop computers must have desktop/laptop firewall software installed on them. • All VPN-connected and dial-up connected workstations that remotely connect to the state's network must have desktop/laptop firewall software installed on them.	S03.002.003	Controls > Control Categories > Technical	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. See FIPS 200.	The current approved and supported enterprise standards for individual computers connecting to the Commonwealth's Intranet are: • McAfee HIPS • Microsoft Windows Firewall • Symantec - Norton Personal Firewall • Zone Labs: Zone Alarm (free for home use); Zone Alarm Plus; Zone Alarm Pro; Zone Labs' enterprise solution includes Zone Labs Integrity, Zone Labs Integrity Desktop, and Integrity Desktop Manager (simple deployment tool).	**Effective:** 12/5/2003 **Revised:** 1/19/2011 **Reviewed:** 6/17/2015